When Does a Polynomial Over a Finite Field Permute the Elements of the Field?
Author(s): Rudolf Lidl and Gary L. Mullen
Source: *The American Mathematical Monthly*, Vol. 95, No. 3 (Mar., 1988), pp. 243-246
Published by: Mathematical Association of America
Stable URL: http://www.jstor.org/stable/2323626
Accessed: 17/09/2014 17:25

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at
http://www.jstor.org/page/info/about/policies/terms.jsp

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

Mathematical Association of America is collaborating with JSTOR to digitize, preserve and extend access to *The American Mathematical Monthly.*

http://www.jstor.org

UNSOLVED PROBLEMS

EDITED BY RICHARD GUY

In this department the MONTHLY *presents easily stated unsolved problems dealing with notions ordinarily encountered in undergraduate mathematics. Each problem should be accompanied by relevant references (if any are known to the author) and by a brief description of known partial results. Manuscripts should be sent to Richard Guy, Department of Mathematics and Statistics, The University of Calgary, Calgary, Alberta, Canada T2N 1N4.*

When Does a Polynomial over a Finite Field Permute the Elements of the Field?

RUDOLF LIDL*
Department of Mathematics, University of Tasmania, Hobart, Tasmania 7001, Australia

GARY L. MULLEN**
Department of Mathematics, Pennsylvania State University, University Park, PA 16802

If $f(x) = a_0 + a_1x + \cdots + a_nx^n$ is a polynomial of degree n over the finite field F_q of order $q = p^\delta$ where p is a prime and $\delta \geqslant 1$, does the associated polynomial function $f\colon c \to f(c)$ from F_q into F_q permute the elements of F_q, i.e., is f a 1-1 map of F_q onto itself? If f is a permutation of F_q then the polynomial $f(x)$ is called a **permutation polynomial** (PP) of F_q. Very little is known concerning which polynomials are PPs, despite the attention of numerous authors (see the notes to Chapter 7 of [**13**]). Very few good algorithms exist to test whether a given polynomial is a PP. We describe several applications of permutations which indicate why a study of permutations is of interest, and we list, without proof, the known classes of PPs and the known criteria. We indicate a number of open problems and make some conjectures.

Recently, permutations of finite fields have become of considerable interest in the construction of cryptographic systems for the secure transmission of data. See, for example [**12**, Chapter 9] and [**10**]–[**11**]. Let M be a message (an element of F_q) which is to be sent securely from A to B. If $P(x)$ is a permutation of F_q, then A sends to B the field element $N = P(M)$. Since $P(x)$ is a bijection, B can obtain the original message M by calculating $P^{-1}(N) = P^{-1}(P(M)) = M$. In order to be useful in a cryptographic system, $P(x)$ must have several additional properties; see problem P3. Cryptographic systems of a different type, based on permutations of finite fields, were considered by Levine and Brawley in [**10**].

*Research was supported by the Australian Research Grants Committee, grant F8415183.

**This author would like to thank the mathematics department at the University of Tasmania for its hospitality during a recent visit when discussions which led to this paper took place.

This content downloaded from 128.62.30.17 on Wed, 17 Sep 2014 17:25:56 PM
All use subject to JSTOR Terms and Conditions

Permutations are also useful in several combinatorial applications. The reader is referred to Theorems 9.67 and 9.83 of [**13**] as well as [**4**] and [**19**]–[**20**] for illustrations thereof.

We now list the major known classes of PPs. If $f(x)$ is a PP of F_q, then so is $f_1(x) = af(x+b)+c$ for all $a \neq 0, b, c \in F_q$ and we say that $f_1(x)$ is in **normalized form** if a, b, c are chosen so that $f_1(x)$ is monic, $f_1(0) = 0$, and (provided the characteristic p does not divide the degree n) the coefficient of x^{n-1} is 0.

(1) In [**5**, p. 63] Dickson lists all normalized permutations of degree at most 5.

(2) x^k permutes F_q if and only if $(k, q-1) = 1$.

(3) If $a \in F_q$, then the Dickson polynomial

$$g_k(x,a) = \sum_{j=0}^{[k/2]} \frac{k}{k-j}\binom{k-j}{j}(-a)^j x^{k-2j}$$

permutes F_q if and only if $(k, q^2-1) = 1$ [**13**, Theorem 7.16].

(4) If F_{q^r} is an extension of F_q of degree r, then $L(x) = \Sigma_{s=0}^{r-1}\alpha_s x^{q^s}$ with $\alpha_s \in F_{q^r}$ is a linear operator on F_{q^r} over F_q and it permutes F_{q^r} if and only if $\det(\alpha_{i-j}^{q^j}) \neq 0$ $(i, j = 0, 1, \dots, r-1)$. If each $\alpha_s \in F_q$ then $L(x)$ permutes F_{q^r} if and only if $(\Sigma_{s=0}^{r-1}\alpha_s x^s, x^r - 1) = 1$ [**13**, pp. 362, 390].

(5) If $r > 1$ is prime to $q-1$, s divides $q-1$, and $g(x^s)$ has no nonzero root in F_q, where $g(x) \in F_q[x]$, then $x^r(g(x^s))^{(q-1)/s}$ permutes F_q [**13**, Theorem 7.10].

(6) Several other specific classes of PPs have been characterized [**13**, Chapter 7], e.g., $x^{(q+m-1)/m} + ax$ where m divides $q-1$ and $x^r(x^d - a)^{(p^n-1)/d}$, where $d|(p^n-1)$.

This list is not exhaustive, but it does contain all known major classes: so we don't have very many types of PPs.

Suppose we wish to determine whether $f(x) = \Sigma_{i=0}^n a_i x^i$ permutes F_q. We may assume that $n \leqslant q-1$ since every function from a finite field F_q to itself can be represented by a polynomial of degree $< q$ [**13**, p. 369]. If q is small, one could proceed by calculating $f(a)$ for all $a \in F_q$ and checking whether the q values $f(a)$ are indeed distinct. However since this involves $O(qn)$ F_q operations for a polynomial f of degree n, this becomes prohibitive if q is large.

The first, and in some ways most useful, criterion was proved by Hermite [**8**] for q prime, and by Dickson [**6**] for general q.

THEOREM. *$f(x)$ permutes F_q if and only if*

(1) *f has exactly one root in F_q and*

(2) *For each integer t with $1 \leqslant t \leqslant q-2$ with $t \not\equiv 0 \pmod p$, the reduction of $[f(x)]^t \bmod (x^q - x)$ has degree $\leqslant q-2$.*

COROLLARY. *If $f(x)$ is a* PP *of F_q of degree $n > 1$, then $n \nmid (q-1)$.*

London and Ziegler [**14**], Raussnitz [**21**], and Mollin and Small [**16**] investigated criteria for $f(x)$ to be a permutation in terms of the coefficients of $f(x)$. Two sufficient conditions can be found in Carlitz and Lutz [**2**].

We now list a number of open problems and conjectures involving PPs of finite fields.

This content downloaded from 128.62.30.17 on Wed, 17 Sep 2014 17:25:56 PM
All use subject to JSTOR Terms and Conditions

P1. Find an algorithm of lower complexity than $O(qn)$ to test whether a given polynomial is a PP of F_q.

P2. Find new classes of PPs of F_q.

P3. Find new classes of permutations $P(x)$ that are useful cryptographically. Hence $P(x)$ should have a simple form so that if M is a message, then $N = P(M)$ which is sent from A to B can be easily computed. Also $P(x)$ must have the property that without some secret information (the key) that only A and B know, $P^{-1}(x)$ will be hard or impossible to get, so that an unauthorized receiver cannot calculate $P^{-1}(N)$. At the same time with knowledge of the key, $P^{-1}(x)$ is easily obtained by B so that $P^{-1}(N) = M$ can be recovered by B.

P4. The Chebyshev polynomial of the second kind of degree k is defined by

$$f_k(x) = \sum_{i=0}^{[k/2]} \binom{k-i}{i}(-1)^i x^{k-2i}.$$

It can be shown that $f_k(x) = xf_{k-1}(x) - f_{k-2}(x)$ for $k \geqslant 2$. For odd q determine necessary and sufficient conditions on k and q so that $f_k(x)$ permutes F_q. In [**15**] Matthews showed that for odd q, if $k + 1 \equiv \pm 2 (\mathrm{mod}\, m)$ for $m = p$, $(q-1)/2$, and $(q+1)/2$, then $f_k(x)$ permutes F_q, and in fact then, $f_k(-a) = -f_k(a)$ and $f_k(a) = \pm a$ for all $a \in F_q$. Based upon computer evidence, we conjecture that if q is prime, then the above conditions are also necessary. Moreover if the characteristic $p > 5$ it appears that the conditions are both necessary and sufficient for $f_k(x)$ to permute F_q. For $p = 3$ and 5, there are examples of $q > p$ and of k such that $f_k(x)$ permutes F_q but k does not satisfy the above set of congruences.

P5. Extend Dickson's list [**5**, Table 7.1] of normalized PPs to higher degrees.

P6. Let $N_d = N_d(q)$ denote the number of PPs of degree d over F_q. We have the trivial boundary conditions $N_1 = q(q-1)$, $N_d = 0$ if $d|(q-1)$, and $\Sigma N_d = q!$ where the sum is over all $1 \leqslant d < q-1$ with $d \nmid (q-1)$. Find N_d. Some partial results in this direction were given in Wells [**24**].

P7. Suppose $f(x)$ is a PP of degree p over F_q. Dickson [**5**] conjectured that $f(x)$ is reducible to the normalized PP $x(x^d - \alpha)^{(p-1)/d}$ where $d|(p-1)$ and $\alpha \neq \beta^d$ for any $\beta \in F_q$, having earlier proved this for $p = 3$, 5, and 7 in his thesis [**6**]. Settle this conjecture for all odd primes p.

P8. Settle the conjecture of Chowla and Zassenhaus [**3**] that if p is a sufficiently large prime and $f(x)$ of degree $\geqslant 2$ permutes F_p, then $f(x) + ax$ with $0 < a < p$ is not a PP of F_p. For several partial results, see [**20**] and [**17**].

P9. In an invited address before the MAA in 1966, Carlitz conjectured that for each even positive integer k, there is a constant C_k such that for each finite field of odd order $q > C_k$, there does not exist a PP of degree k over F_q. Lausch and Nöbauer [**9**, p. 202] proved the conjecture for $k = 2^m$ and for $k = 6$ and 10 the conjecture has been proven by Dickson [**6**] and Hayes [**7**], respectively. Recently Wan Daqing [**22**] settled the cases $k = 12$ and 14. A major result would be a proof of the Carlitz conjecture for arbitrary even k.

Many similar questions can be considered for polynomials in several variables over F_q, see e.g. [**13**, Sect. 7.5] and for residue class rings of integers, see for example [**9**] and [**18**], where there are numerous other references.

This content downloaded from 128.62.30.17 on Wed, 17 Sep 2014 17:25:56 PM
All use subject to JSTOR Terms and Conditions

Acknowledgment. The authors would like to thank the referee and the editor for a number of suggestions that improved the final version of the paper.

REFERENCES

1. L. Carlitz, Permutations in a finite field, *Acta Sci. Math. Szeged*, 24 (1963) 196–203.
2. L. Carlitz and J. A. Lutz, A characterization of permutation polynomials over a finite field, this MONTHLY, 85 (1978) 746–748.
3. S. Chowla and H. Zassenhaus, Some conjectures concerning finite fields, *Norske Vid. Selsk. Forh.* (Trondheim), 41 (1968) 34–35.
4. S. D. Cohen and M. J. Ganley, Some classes of translation planes, *Quart. J. Math.*, *Oxford Ser.*, (2) 35 (1984) 101–113.
5. L. E. Dickson, Linear Groups with an Exposition of the Galois Field Theory, Teubner, Leipzig, 1901; Dover, New York, 1958.
6. L. E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, *Ann. of Math.*, 11 (1897) 65–120, 161–183.
7. D. R. Hayes, A geometric approach to permutation polynomials over a finite field, *Duke Math. J.*, 34 (1967) 293–305.
8. C. Hermite, Sur les fonctions.de sept lettres, *C. R. Acad. Sci. Paris*, 57 (1863), 750–757; Oeuvres, vol. 2, Gauthier-Villars, Paris, 1908, 280–288.
9. H. Lausch and W. Nöbauer, Algebra of Polynomials, North-Holland, Amsterdam, 1973.
10. J. Levine and J. V. Brawley, Some cryptographic applications of permutation polynomials, *Cryptologia*, 1 (1977) 76–92.
11. R. Lidl and W. B. Müller, A note on polynomials and functions in algebraic cryptography., *Ars Combin.*, 17A (1984) 223–229.
12. R. Lidl and H. Niederreiter, Introduction to Finite Fields and their Applications, Cambridge University Press, Cambridge, 1986.
13. R. Lidl and H. Niederreiter, Finite Fields, Encyclopedia Math. Appl., Vol. 20, Addison-Wesley, Reading, Mass 1983 (now distributed by Cambridge Univ. Press).
14. D. London and Z. Ziegler, Functions over the residue field modulo a prime, *J. Austral. Math. Soc.*, *Ser. A* 7 (1967) 410–416.
15. R. W. Matthews, Permutation Polynomials in One and Several Variables, Ph.D. Dissertation, University of Tasmania, 1982.
16. R. A. Mollin and C. Small, On permutation polynomials over finite fields, *Internat. J. Math. Math. Sci.*, 10 (1987) 535–544.
17. G. L. Mullen and H. Niederreiter, Dickson polynomials over finite fields and complete mappings, *Canad. Math. Bull.*, 30 (1987) 19–27.
18. W. Narkiewicz, Uniform Distribution of Sequences of Integers in Residue Classes, Lecture Notes in Math., Vol. 1087, Springer-Verlag, New York, 1984.
19. H. Niederreiter and K. H. Robinson, Bol loops of order pq, *Math. Proc. Cambridge Philos. Soc.*, 89 (1981) 241–256.
20. H. Niederreiter and K. H. Robinson, Complete mappings of finite fields, *J. Austral. Math. Soc.*, Ser A 33 (1982) 197–212.
21. G. Raussnitz, *Math. Naturw. Ber. Ungarn*, 1 (1882/83) 266–278.
22. Wan Daqing, On a conjecture of Carlitz, *J. Austral. Math. Soc.*, *Ser. A* (43) 1987, 375–84.
23. C. Wells, Groups of permutation polynomials, *Monatsh. Math.*, 71 (1967) 248–262.
24. C. Wells, The degrees of permutation polynomials over finite fields, *J. Combinatorial Theory*, 7 (1969) 49–55.

This content downloaded from 128.62.30.17 on Wed, 17 Sep 2014 17:25:56 PM
All use subject to JSTOR Terms and Conditions